electronics

MDPI

Article

Nonlinear Controller-Based Mitigation of Adverse Effects of Cyber-Attacks on the DC Microgrid System

Mohd. Hasan Ali [1,*] and Sultana Razia Akhter [2]

[1] Department of Electrical and Computer Engineering, The University of Memphis, TN 38152, USA
[2] American Express, 18850 N 56th St., Phoenix, AZ 85054, USA
* Correspondence: mhali@memphis.edu

Abstract: Cyber-attacks have adverse impacts on DC microgrid systems. Existing literature shows plenty of attack detection methods but lacks appropriate mitigation and prevention approaches for cyber-attacks in DC microgrids. To overcome this limitation, this paper proposes a novel solution based on a nonlinear controller to mitigate the adverse effects of various cyber-attacks, such as distributed denial of service attacks and false data injection attacks, on various components of a DC microgrid system consisting of a photovoltaic power source, a permanent magnet synchronous generator-based variable speed wind generator, a fuel cell, battery energy storage, and loads. To demonstrate the effectiveness of the proposed solution, single and repetitive cyber-attacks on specific components of the microgrid have been considered. An index-based quantitative improvement analysis for the proposed control method has been made. Extensive simulations have been performed by the MATLAB/Simulink V9 software. Simulation results demonstrate the effectiveness of the proposed nonlinear controller-based method in mitigating the adverse effects of cyber-attacks. Moreover, the performance of the proposed method is better than that of the proportional-integral controller. Due to the simplicity of the proposed solution, it can easily be implemented in real practice.

Keywords: cyber-attack; DC microgrid security; DDoS; FDI; nonlinear controller; mitigation

check for updates

Citation: Ali, M.H.; Akhter, S.R. Nonlinear Controller-Based Mitigation of Adverse Effects of Cyber-Attacks on the DC Microgrid System. *Electronics* **2024**, *13*, 1057. https://doi.org/10.3390/electronics13061057

Academic Editors: Mario Di Ferdinando, Carlo Olivieri and Yassine Chaibi

Received: 24 January 2024
Revised: 7 March 2024
Accepted: 10 March 2024
Published: 12 March 2024

Copyright: © 2024 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

1. Introduction

The microgrid (MG) power system concept has gained wider popularity in recent times due to its localized, autonomous, and resilient power supply [1–7]. Besides the increasing demand for direct current loads (DC-loads), the simplified interface with renewable power generation, the reduction of usage and losses associated with power converters, and the perception that DC microgrid (DC MG) could be a cheaper and more efficient alternative for power supply in small-scale areas like residential areas, university campuses, offices, shopping malls, military bases, aircraft, etc.

Again, the entire DC MG can be monitored by the supervisory control and data acquisition (SCADA) system that stores, monitors, and processes all the data related to the power network, which necessitates multilevel controls for providing reliability and dynamic response for the DC MG system. This multilevel monitoring and control requires two-way communication among the main grid, DC MG, and the SCADA system, which eventually makes the total structure a cyber-physical system. By introducing communication channels with a computerized control system, the functionality and efficiency of the smart power network can be enhanced with a dynamic demand management system. But, this potentiality can introduce the security vulnerability of such a cyber-physical system.

Recently, lots of research has been conducted on detecting and managing the risk of cyber-attacks in power systems [8–11]. The work in [6] describes the security vulnerabilities of smart power systems, especially the DC MG, and discusses some possible forms of attacks such as masquerading, message reply attacks, eavesdropping, false data injection (FDI), distributed denial-of-service (DDoS), and privacy leakage on the smart meters.

Beg et al. propose a method of FDI attack detection in the DC MG system [12]. Likewise, a data-driven approach to distinguishing between cyber-attacks and physical faults using a sequential minimal optimization-based support vector machine has been used in [13]. For FDI attacks, different dynamic state estimation-based detection methods have been broadly discussed in several literatures using deep learning [14], phasor measurement unit data [15], the Chi-square method and Euclidean distance detector [16], the Markov model for determining the state space decision [17], the anomaly detection algorithm [18], and the harmony search algorithm using the K-nearest neighbor [19]. Some other techniques, such as the Diagnostic Robust Generalized Potential technique [20], distributed block chain-based protection framework against DDOS attack through the communicating channel [21], and a parametric feedback linearization-based control scheme for delay minimization due to DDoS attack [22], show effective responses for the power grids.

From the thorough literature search, it appears that the appropriate techniques to mitigate the adverse effects of cyber-attacks on the DC MG are lacking. Moreover, till now, the cyber-attacks that occur only once in a system have been discussed. However, there can be repetitive attacks as well. That means, once an attack has been mitigated, another attack can affect the system one more time. It can continue for a long time, and the whole power system may exhaust and fail.

Based on the above background, this paper proposes new and effective control means in the form of a nonlinear controller to mitigate the adverse effects of cyber-attacks on various components of the DC MG. A DC MG model consisting of a photovoltaic (PV) system, fuel cell, battery energy storage, and a permanent magnet synchronous generator (PMSG)-based variable-speed wind generator system has been developed. Two types of cyber-attacks have been considered in this work, i.e., the DDoS attack, which exhausts system resources by sending flood requests to prevent legitimate users from accessing the system, and the FDI attack, where an intruder aims to attack any data as long as it can result in a wrong estimation for the state variables of a system [23–27]. The reason to choose these two specific cyber-attacks is that, in a recent study [28], it is mentioned that the DDoS attacks affect 80% of the electrical enterprises [29] in 14 countries and thus are one of the most severe attacks [30]. Moreover, the work in [31] states that the FDI is a threatening attack that may cause energy theft by end users, false dispatch on the distribution process, and device breakdown during power generation.

Four parameters, such as the duty cycle of the DC-DC boost converter of the PV system, the reference value of the firing-angle controller of the AC-DC inverter of the PMSG-based wind generator, the reference value of the battery energy management system controller, and the load profile, have been chosen as the cyber-attack points. To demonstrate the effectiveness of the proposed solution in more detail, the mentioned two cyber-attacks in the form of single and repetitive attacks at specific components of the microgrid have been considered. Extensive simulations have been performed by the MATLAB/Simulink V9 software.

The novelty and main contributions of this paper can be summarized as follows:

(i) Development of a new nonlinear controller to mitigate the adverse effects of cyber-attacks on the DC microgrid system.
(ii) Consideration of both single and repetitive attacks on the microgrid system.
(iii) Performance comparison between the proposed nonlinear controller and a proportional-integral (PI) controller for cyber-attack mitigation.

The organization of the paper is as follows: Section 2 describes the cyberphysical modeling of the DC MG system to analyze the cybersecurity issues and solution techniques. Also, this section explains the cybersecurity aspects of the DC MG system. Moreover, a detailed description of the proposed controller and control algorithm for cyber-attack mitigation has been provided in this section. Section 3 shows and describes the simulation results and the effectiveness of the proposed mitigation technique. Finally, Section 4 provides some conclusions for the proposed work.

2. Materials and Methods

2.1. Cyberphysical Modeling of a DC Microgrid System

For the simulation, the system as shown in Figure 1 has been considered, where there is a solar panel with the Perturb and Observatory-based Maximum Power Point Tracking (MPPT) system [32] that produces the duty cycle for the boost converter and provides power to the DC grid. A battery energy storage system (BESS) is also equipped to minimize power fluctuation due to temperature and solar irradiation change [33]. Moreover, a proton exchange membrane-based fuel cell (FC) [34] connected with a DC-DC converter, a PMSG-based variable-speed wind power system (WPS) [35] equipped with an AC-DC inverter, and a DC load are connected with the DC bus that consumes 5.12 MW of power at 400 V. The power capacities of the PV, FC, and WG are 3 MW, 112.5 KW, and 2 MW, respectively. The designed DC bus is connected to the main grid via an inverter through a switching mechanism that ensures bidirectional power flow to and from both grids. The whole DC MG is controlled and monitored through the centralized control system, i.e., the SCADA, in different layers. Cyber-attacks may happen at any point of supervisory control.

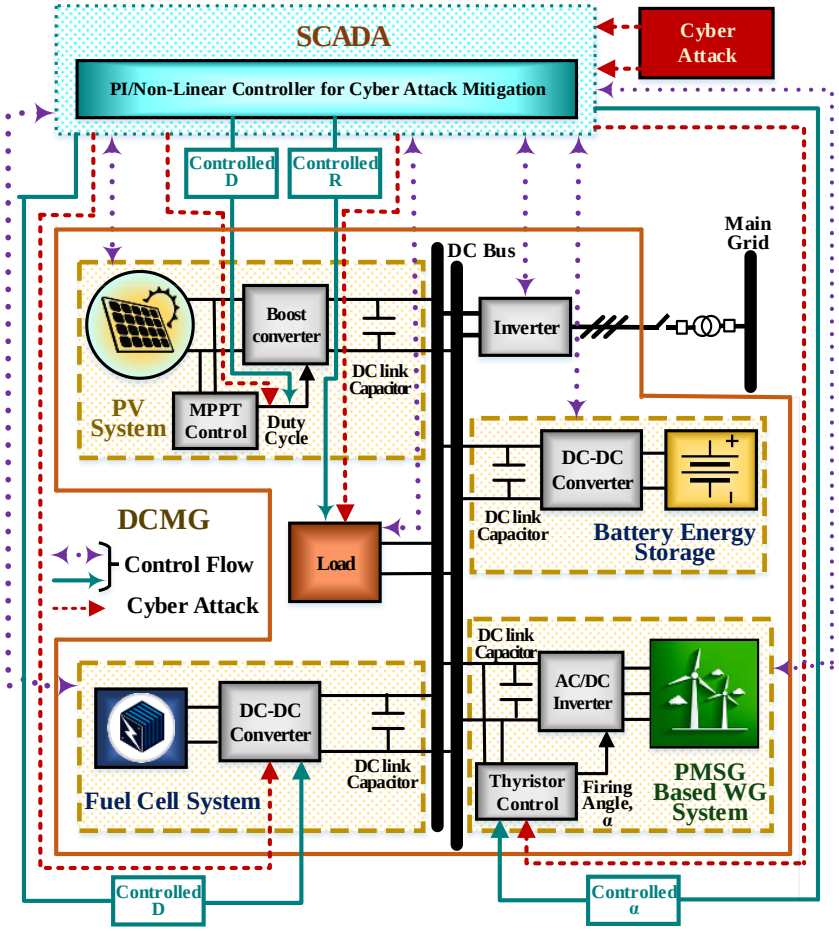

Figure 1. DC microgrid system supervised by the SCADA system.

2.2. Possible Cyber Threats in the DC Microgrid System

As shown in Figure 1, the DC MG is connected to the main grid system, and the total cyberphysical system is being monitored by the SCADA system in different layers. As all the controller set points are handled through the SCADA, it is possible to tamper with any kinds of data from there or destroy the interface with the grid, which may result in an unexpected and unbalanced situation. For example, an intruder can change the value of the duty cycle, which is the input to the boost converter of the PV system, abruptly to any value. Information on the duty cycle can be missing from the boost converter. Again,

an attacker can attack the load profile, which will cause a change in the load value at the SCADA, whereas the physical load value will remain unchanged. In all of these cases, the physical system will receive misleading information from the SCADA, which will result in a deviation of the PV array terminal voltage and the voltage and power at the DC MG terminal.

Moreover, since every controller has some reference values, an intruder can easily change that set point, which can hamper the performance of the controller. For example, in the BESS, an intruder can change the reference value of the power. In that case, the controller will not be able to provide the optimum power required for the system at that moment, and that will hamper the performance of the power system, and the consumers will also be affected by the high or low voltage caused by the variable nature of the solar or wind. If such a situation continues for a longer time, the equipment attached to the power system will be damaged, and the whole system may be shut down. Table 1 shows the potential cyber threat and its impact on the overall DC microgrid system.

Table 1. Potential cyber threat and its impact on the DC microgrid.

Type of Attack	Nature of the Attack	Device Affected by the Attack	Effect on the Device	Overall Consequence on the Microgrid
FDI	Intruder manipulates the controller parameters	Inverter, Converter, Thyristor controller, and MPPT controller	Changes in voltage and power cause cascading effects on other devices.	System shutdown and may cause equipment damage as well. Results in an overall socio-economic imbalance.
	Intruder tampers with the load profile	Load		
DDoS	Disrupts the normal data flow, resulting in delays in the system	Inverter, Converter, Thyristor controller, and MPPT controller		

2.3. Distinguishing Cyber-Attacks from Other Disturbances

As already mentioned, to consider the cyber-attack scenario, in this work four parameters have been chosen, i.e., the duty cycle of the PV system, the reference value of the firing-angle controller of the PMSG-based wind generator, the reference value of the BESS control scheme, and the load profile. All these quantities are independent of the fault or any other transient instability scenario on the grid. The duty cycle usually varies with the change in solar irradiance and the temperature to obtain the maximum power point in the case of the PV system or with the fuel cell dynamics in the case of the FC system. This type of variation is time-dependent and does not change instantly or abruptly. Again, during a fault condition, the reference values of the controller never change unless those are manipulated intentionally. Similarly, in the case of a load, its value never varies with the fault. The only parameter that can vary is the voltage, which may go very low, and the current, which may become very high during the fault. The value of the load may vary with respect to the demand throughout the day, but this will not happen abruptly or enormously, as the load profile is always maintained and monitored according to the grid code by the SCADA. Whereas in the case of an FDI cyber-attack, the parameters can be changed to very sudden and unusual values, or in the case of a DDoS attack, due to the flood of data, some delayed response may occur. Therefore, by recognizing the pattern of the duty cycle and load profile along with monitoring the reference values of each controller at the SCADA, the cyber-attack scenarios can possibly be recognized.

2.4. Modeling of Cyber-Attacks

As already mentioned, this work has considered two types of cyber-attacks, such as FDI and DDoS attacks. A detailed description of the attacks and their modeling are discussed below.

2.4.1. False Data Injection (FDI) Attack Model

FDI attack refers to adding an attack vector (c) to the control vector (z), resulting in a manipulated control vector (z_c), as shown in Equation (1).

$$z_c = z + c \tag{1}$$

The FDI detection problem can be thought of as a binary classification problem from a machine-learning standpoint. Let samples with M characteristics from either c (negative class) or ca be the measurement data (positive class). The definition of the matching class labels, y, is given in Equation (2):

$$y = \begin{cases} +1\,; if\ c \neq 0 \\ -1\,; if\ c = 0 \end{cases} \tag{2}$$

The distance between two arbitrary samples, s_i and s_j, without losing generality, is provided by Equations (3)–(5) [36]:

$$\left\| s_i - s_j \right\|_2 = \begin{cases} \left\| z_i - z_j + c_i\ - c_j \right\|_2 ; if\ c_i\ ,\ c_j\ \neq 0 \\ \left\| z_i - z_j + c_i \right\|_2 ; if\ c_i\ \neq 0, c_j = 0 \\ \left\| z_i - z_j \right\|_2 ; if\ c_i\ ,\ c_j\ = 0 \end{cases}$$

FDI attacks can result in a change in the duty cycle of the PV boost converter and the load profile, which can impact the overall power system.

2.4.2. Distributed Denial of Service (DDoS) Attack Model

In DDoS attacks, the attacker targets the communication links of the system and makes them jammed. As a result, communication becomes slow or completely stopped. Since the communication network is of extreme significance in the PV system, DDoS attacks have a very disruptive impact on the system. Equations (6) and (7) present the original control signal and delayed signal, respectively, if the communication delay in the network produced by a DDoS attack is N_0 [37].

$$x_{original}\ (t) = x(t) = \sum_{i=0}^{N} x_i \tag{6}$$

$$x_{delay}\ (t) = x(t - N_o) = \sum_{i=-N_o}^{N-N_o} x_i \tag{7}$$

Equation (8) illustrates that adding N_0 sample time to the current timestep x_{delay} is needed to obtain the same sample from the original control signal $x_{original}$.

$$x_{delay}\ (t + N_0) = x_{original}\ (t) \tag{8}$$

This is what the DDoS attack sequence looks like: (a) According to (9a), the PV system functions normally, that is, it communicates with remote SCADA and other controllers in a normal manner. (b) Suddenly, at sample time $t_1 \geq 0$ and continuing until $t_2 = t_1 + N_0 \leq N$, where N_0 is the delay that varies depending on the intensity of the DDoS attack. According to (9b), the signal is completely lost during this time, or zero. (c) The signal should maintain the t_1 + 1 signal sample as in (9c) in post-attack because DDoS should not jeopardize the signal's integrity. The composite control signal that reaches the PV controller can be expressed as (9).

$$x(t) = \begin{cases} x_{original}\ (t)\ if\ 0 \leq t < t_1,\ pre\ attack & \text{(9a)} \\ 0\ if\ t_1 < t < t_2, attack & \text{(9b)} \\ x_{delay}\ (t)\ if\ t_2 < t < N,\ post\ attack & \text{(9c)} \end{cases}$$

2.5. Proposed Nonlinear Control Methodology for Cyber-Attack Mitigation

In this work, a nonlinear controller-based approach has been used to mitigate the adverse effects of cyber-attacks on the performance of the microgrid system. The control algorithm and the controller description are provided in the following:

2.5.1. Control Algorithm

All kinds of vulnerabilities in a power system have a direct impact on the terminal voltage. Therefore, the main objective is to regain the voltage at its required level within the shortest possible time. Thus, the DC link voltage (V_{DC}) has been used as the controller input. This voltage is compared with the reference voltage of V_{DC} (400 V) to obtain the error function ΔV_{DC}. Figure 2 shows the flowchart of the basic algorithm of the proposed cyber-attack mitigation techniques.

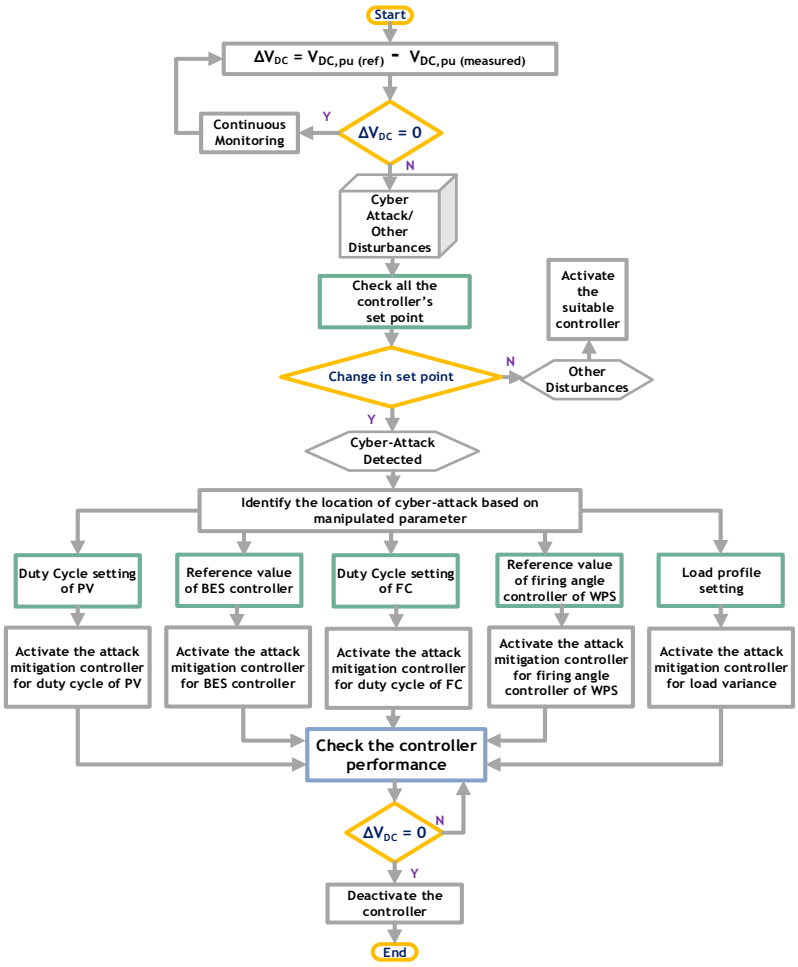

Figure 2. Flowchart of the proposed control algorithm.

In a normal situation, the error value is zero. The controller continuously monitors the voltage deviation on the DC bus. In case of any deviation in ΔV_{DC}, the controller will first check all the set point values to determine whether there is any cyber-attack or any other disturbances in the system. If the set point values are unchanged, then this will indicate the occurrence of other disturbances, and accordingly, a suitable controller will be activated. But, if any of the set point values is changed, then this will ensure the occurrence of a cyber-attack. In this work, as the main focus is to mitigate the adverse effects of cyber-attacks, the control algorithm will check for the location of the cyber-attack depending upon the manipulated parameter. This can be detected by monitoring the performances of the individual distributed energy resources (DER), because the cyber-attack impact will be higher on that specific DER where the attack has occurred. Again, if there is any deviation

in the load value, R, then the controller for the R value correction will be enabled and will ensure the voltage deviation is zero. When the system becomes stable, the controller will be disconnected immediately, and the system will resume its original status.

2.5.2. Nonlinear Controller

As the power grid is highly nonlinear, the application of nonlinear controllers is highly preferred. This control action can be governed by any nonlinear differential equation or any other mathematical model. In this work, an exponential equation has been used as the nonlinear controller function, as shown in the following:

$$D/R = 1 - K_2 e^{-|\Delta V_{DC}|K_1} \tag{10}$$

where K_1 and K_2 are the constant values, and ΔV_{DC} and D/R are the input and output variables of the controller, respectively. Equation (10) is used for cyber-attack mitigation in the case of the load (resistance value, R) and duty cycle, D, of the PV system. By tuning the values of K_1 and K_2, the required controlled values of the manipulated signal are obtained. The parameters have been set in such a way that the controller can handle any kind of voltage deviation, from very high to very low. The parameters of the controller have been shown in Table 2.

Table 2. Parameter values of the controllers.

Attack Point	Nonlinear Controller		PI Controller	
	K_1	K_2	K_p	K_i
D of PV	0.735	0.5	0.9972	0.896
R	0.0215	0.9468	0.34	0.09

2.6. PI Controller for Cyber-Attack Mitigation

In this work, the performance of the proposed nonlinear controller-based attack mitigation approach has been compared with that of a PI-based controller. The PI is one of the popular controllers that is extensively used in industrial control systems. The transfer function that has been used for the PI controller in Laplace domain (s) is as follows:

$$D/R = |\Delta V_{DC}| \left[K_p + \frac{1}{s} K_i \right] \tag{11}$$

where K_p and K_i are the proportional and integral gains of the PI controller, respectively. ΔV_{DC} and D/R are the input and output variables of the controller, respectively, and bear the same meaning as mentioned in the previous subsection. The values of the parameters K_p and K_i are shown in Table 2. These values have been obtained by trial and error, and they can handle any abrupt change in the input from high to low values. For tuning these K_1, K_2, K_p, and K_i parameters using the trial-and-error method, we experimented with a range of values from 0 to 1 with an interval of 0.0001 and observed the performance. Hence, the values mentioned in Table 2 gave us the best and most consistent results for the system.

3. Results and Discussion

In this section, the effectiveness of the proposed controller in the DC microgrid system has been evaluated. The evaluation has been shown through some graphical images obtained from the real-time simulation and also mathematically by calculating the percentage improvement from the voltage index value. The details are described in the following subsections:

3.1. Simulation Condition

The simulations are performed through the MATLAB/Simulink software. In the simulation study, we've considered constant irradiance and temperature in the PV system and constant wind speed in the wind power system, as these parameters vary gradually

with time and any cyber-attack may happen within a few seconds, so these changes will not impact much. In all cyber-attack cases, we have activated the mitigation controller after 0.1 s of the occurrence of the attack. This 0.1 s time has been considered a time delay to allow the sensor to choose the right type of controller based on the location of the attack to mitigate the adverse effects of cyber-attacks. The time step of the simulation is 5 µs for all cases. The scenarios that have been considered in this work are briefly listed in the following Table 3 based on the pattern, type, and location of the attack.

Table 3. Cyber-attack scenario.

Case of Study	Scenario	Pattern of Attack	Type of Attack	Location of Attack
Case-I Attack on PV System	1	Single Attack	FDI	Duty Cycle of the PV Boost Converter
	2		DDoS	
	3	Random Attack	FDI	
Case-II Attack on Load Profile	1	Single Attack	FDI	Load Profile

3.2. Analysis of Cyber Security Issues and Solutions for DC Microgrid Systems

3.2.1. Cyber-Attack on the PV System

CASE-I, SCENARIO-1 (Effects and Solution of the FDI Attack on the Duty Cycle of the PV Boost Converter)

In the case of the false data injection attack scenario, it has been considered that, at 0.5 s of simulation, the intruder attacks the duty cycle at the input of the DC-DC boost converter. Figures 3–6 show the responses of four parameters, such as the duty cycle, PV array voltage, DC grid voltage, and output power, respectively. As shown from the responses, the duty cycle increases to its 90% value, which is a very high value as its range typically may vary from 0 to 1. Also, the terminal voltage of the PV array goes close to zero, and the DC grid voltage and the power at the grid become very low.

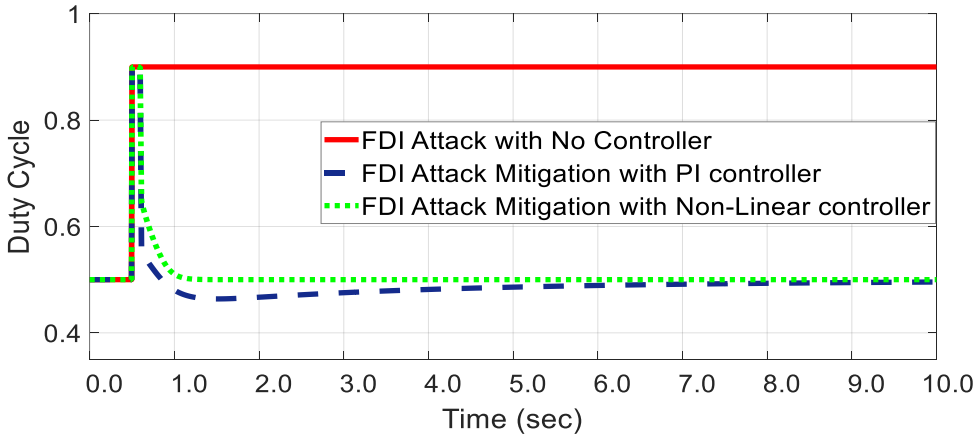

Figure 3. FDI attacks on the duty cycle of the PV boost converter scenario and mitigation effects on the duty cycle.

In that situation, to recover the steadiness of the grid, the controller has been activated at 0.6 s. For the PI controller case, the duty cycle comes back to 0.5 within almost 6 s, compared to that in the case of the nonlinear controller, where the duty cycle comes back to the desired value immediately, within 1 s. As the D value is recovered, both the voltages at the terminal of the PV array and the DC grid gradually come back to the 400 V level. Following the voltage, the output power is also improved. It is quite certain that in all four cases, the performance of the nonlinear controller is much better than that of the PI controller.

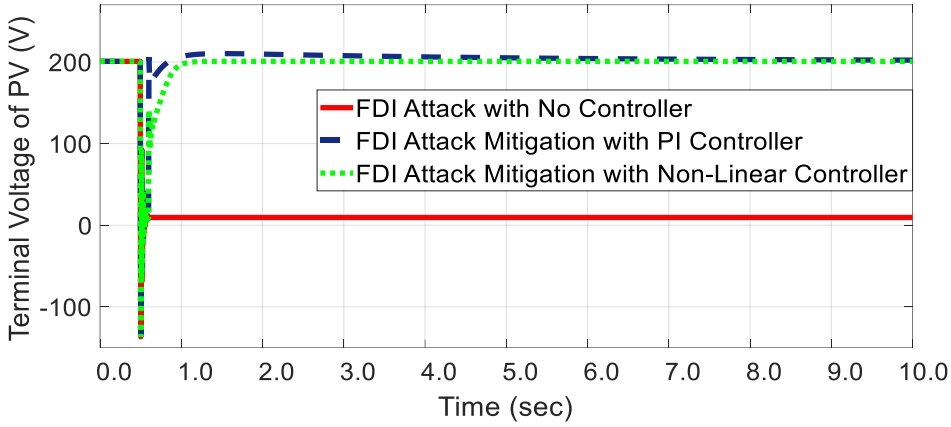

Figure 4. FDI attacks on the duty cycle of the PV boost converter scenario and mitigation effects on the PV array terminal voltage.

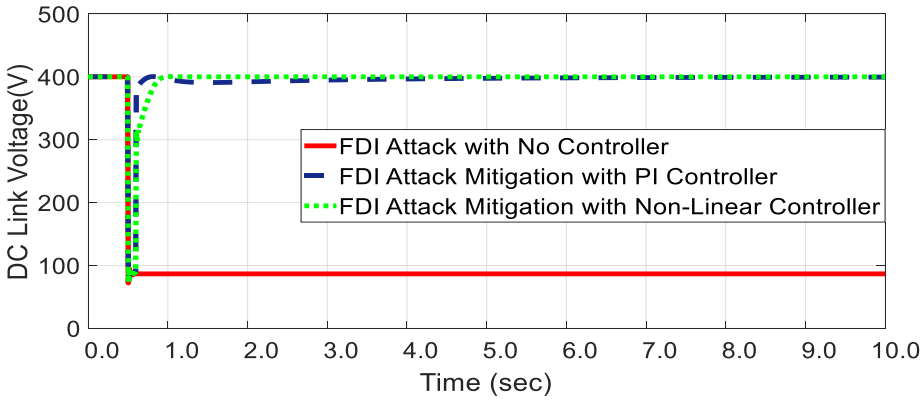

Figure 5. FDI attack on the duty cycle of the PV boost converter scenario and mitigation effects on the DC microgrid terminal voltage.

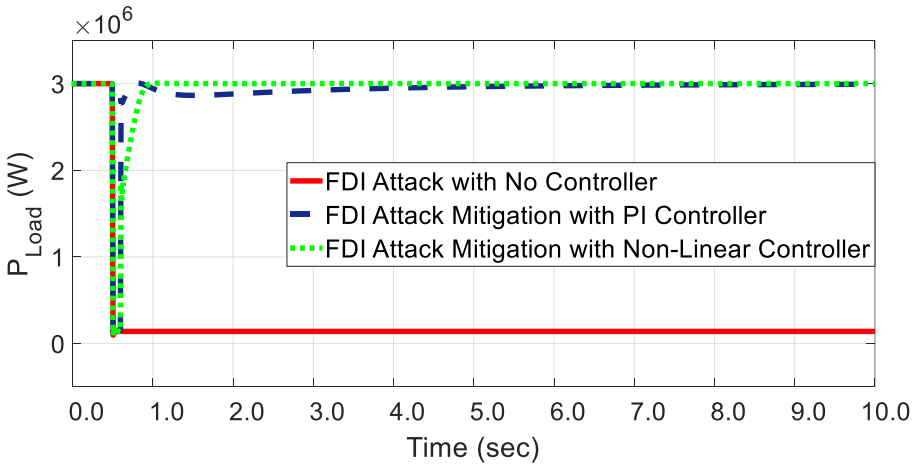

Figure 6. FDI attack on the duty cycle of the PV boost converter scenario and mitigation effects on the power at DC microgrid.

CASE-I, SCENARIO-2 (Effects and Solution of the DDOS Attack on the Duty Cycle of the PV Boost Converter)

The DDoS is another very frequent type of cyber-attack. It causes floods of data that prohibit normal data flow through the communication channel. Therefore, the system will receive no signal for a few moments or a longer period of time. In the case of the DDoS attack, the scenario has been simulated as the intruder attacks the duty cycle by making it

zero in the boost converter input at 0.5 s. Figures 7–10 show the responses of the duty cycle, voltage at both the terminal of the PV array and the DC grid, and load power, respectively. From these figures, it is clear that the sudden absence of duty cycle in the DC-DC Boost converter makes the system vulnerable, as the DC grid voltage and PV array terminal have been activated to handle such a situation. The controller has been activated at 0.6 s, and both controllers attempt to make the duty cycle value at 0.5 at the terminal of the boost converter.

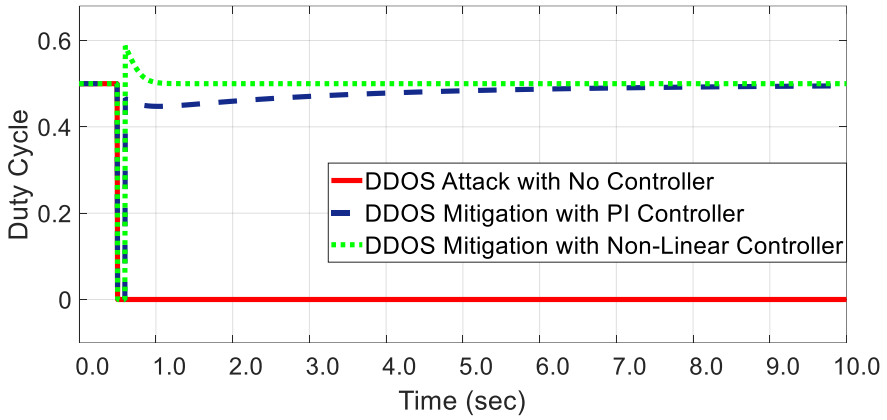

Figure 7. DDoS attacks on the duty cycle of the PV boost converter scenario and mitigation effects on the duty cycle.

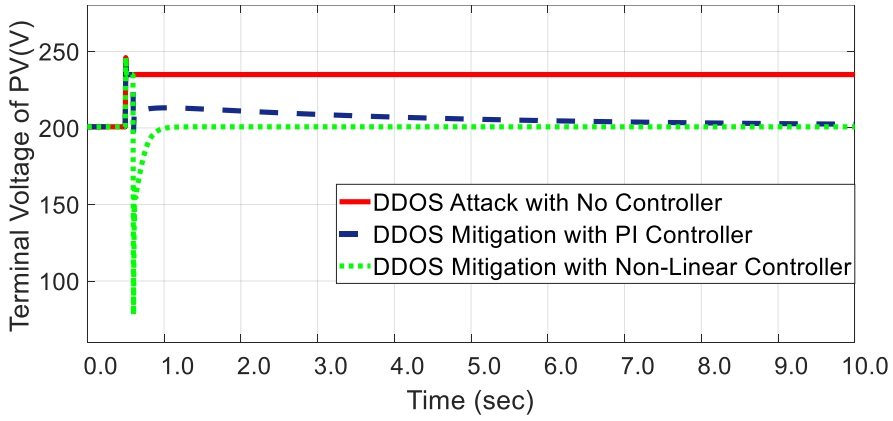

Figure 8. DDoS attack on the duty cycle of the PV boost converter scenario and mitigation effects on the PV array terminal voltage.

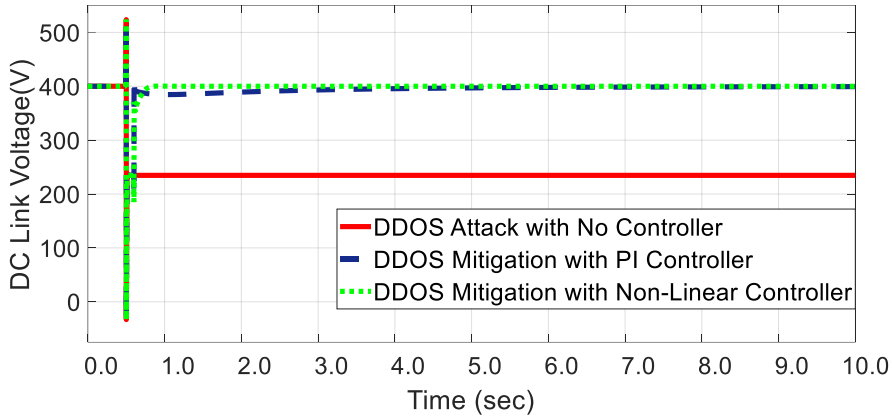

Figure 9. DDoS attack on the duty cycle of the PV boost converter scenario and mitigation effects on the DC microgrid terminal voltage.

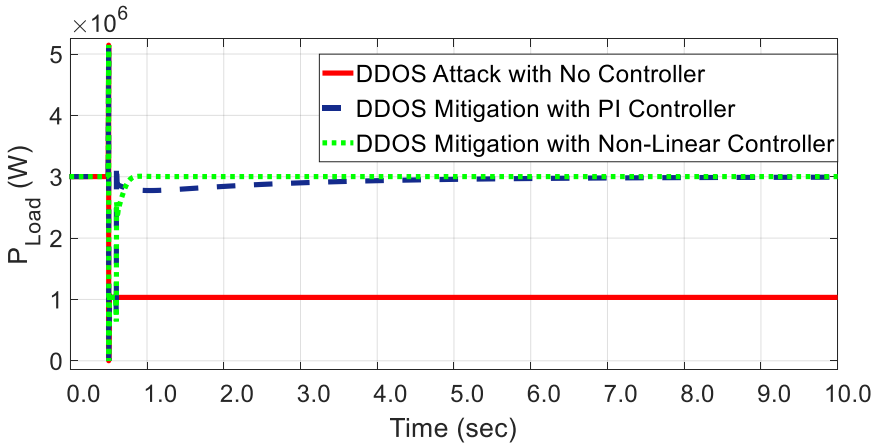

Figure 10. DDoS attack on the duty cycle of the PV boost converter scenario and mitigation effects on the power at the DC microgrid.

From Figures 7–10, it is evident that the performance of the nonlinear controller and the PI controller is significantly different. For every case, the nonlinear controller performs almost instantly after the activation and helps the duty cycle and DC grid voltage come back instantly at their rated values of 0.5 and 400 V, respectively. But, in the case of the PI controller, the duty cycle value was restored almost after 7 s, and the PV array voltage took a long time to become stable, although the DC grid terminal voltage and the output power came back after 5 s.

CASE-I, SCENARIO-3 (Effects and Solution of Random FDI Attack on Duty Cycle of the PV Boost Converter)

In the case of the random false data injection attack scenario, it has been considered that, at 0.5 s of simulation, the intruder attacks with a random change in value of the duty cycle at the input of the DC-DC boost converter of the PV system. Figures 11–14 show the responses of four parameters, such as the duty cycle, PV array voltage, DC grid voltage, and output power. As shown from the responses, the duty cycle varies randomly within a 10–90% value range. Also, the terminal voltage of the PV array, the DC grid voltage, and the power at the grid vary randomly from very low to very high values in an inversely proportional manner with the duty cycle change.

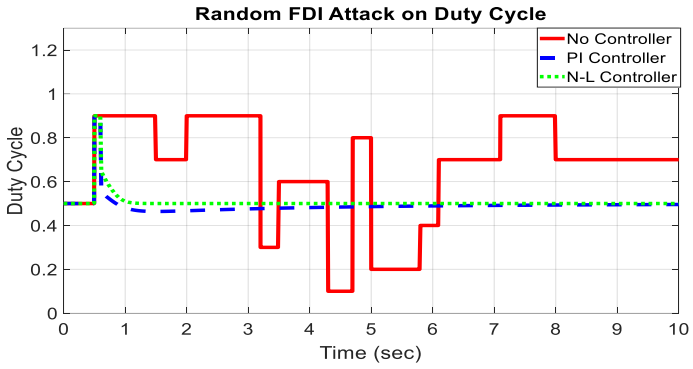

Figure 11. Random FDI attack on the duty cycle of the PV boost converter scenario and mitigation effects on the duty cycle.

In that situation, to recover the stability of the grid, the controller has been activated at 0.6 s. For the PI controller case, the duty cycle comes back to 0.5 within almost 6 s, compared to that in the case of the nonlinear (N-L) controller, where the duty cycle comes back to the desired value immediately, within 1 s. As the D value is recovered, both the voltages at the terminal of the PV array and the DC grid gradually come back to the 400 V

level. Following the voltage, the output power is also improved. It is quite certain that in all four cases, the performance of the nonlinear (N-L) controller is much better than that of the PI controller. This proves the robustness of the controllers, which means they can handle any abrupt changes properly within a very short period of time.

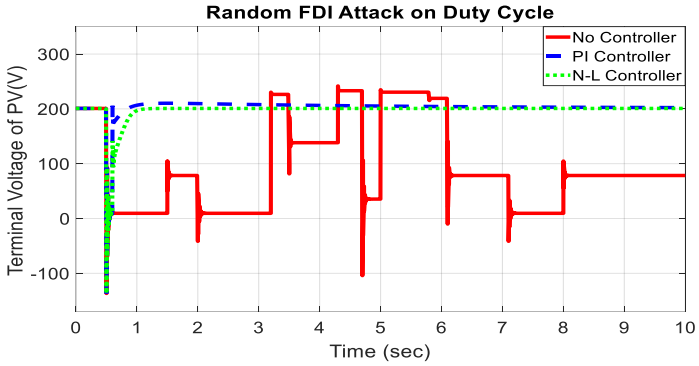

Figure 12. Random FDI attack on the duty cycle of the PV boost converter scenario and mitigation effects on the terminal voltage of the PV array.

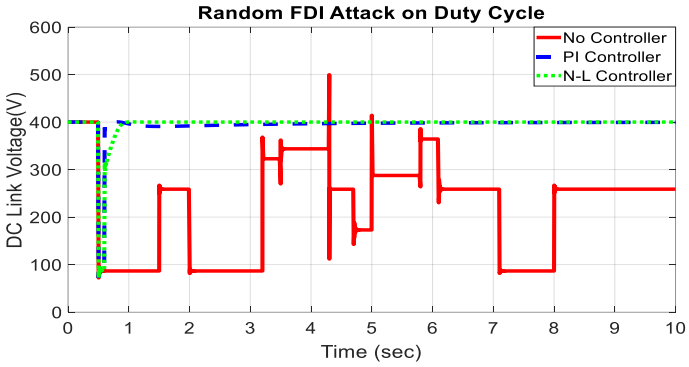

Figure 13. Random FDI attack on the duty cycle of the PV boost converter scenario and mitigation effects on the voltage at the DC link.

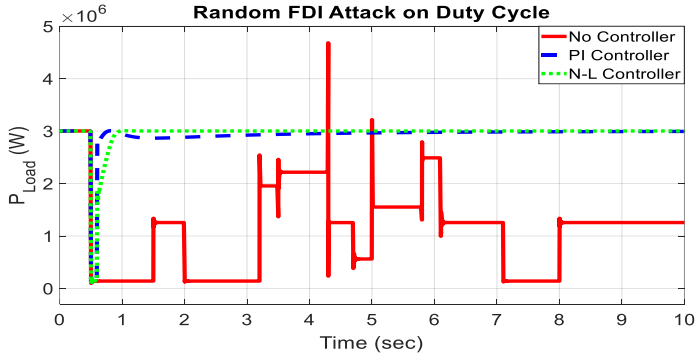

Figure 14. Random FDI attack on the duty cycle of the PV boost converter scenario and mitigation effects on the load power.

3.2.2. Cyber-Attack on Load Profile

CASE-II, SCENARIO-1 (Effects and Solution of FDI Attack on Load)

In this case, the attack has been simulated in such a way that at 0.5 s, the intruder changes the value of the load from the original set value of 0.0533 Ω to a high value of 0.3 Ω. For such a high load value, the terminal voltage of the DC grid rises to 558.4 V. As a result, the maximum power point condition becomes diverged, and the power goes very low. And the system becomes unstable. In this situation, at 0.6 s, the controllers have been

activated to stabilize the system by setting back the load. Figures 15–18 show the responses of the duty cycle, voltage at both the terminal of the PV array and the DC grid, and load power, respectively.

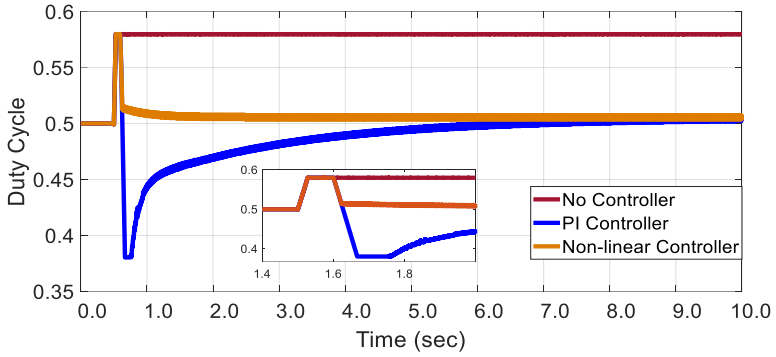

Figure 15. FDI attack on the load scenario and mitigation effect on the duty cycle.

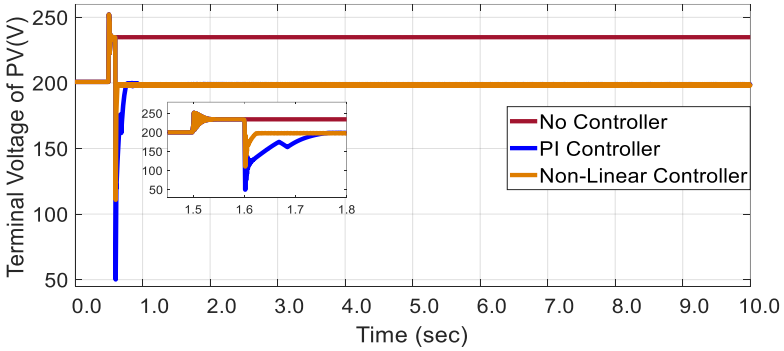

Figure 16. FDI attack on the load scenario and mitigation effect on the PV array terminal voltage.

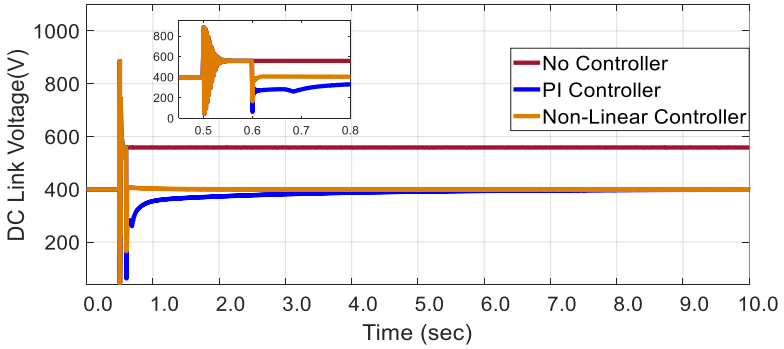

Figure 17. FDI attack on the load scenario and mitigation effect on the DC microgrid terminal voltage.

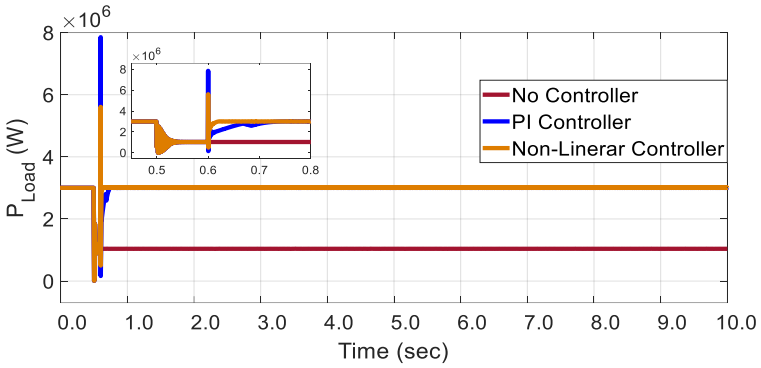

Figure 18. FDI attack on the load scenario and mitigation effect on the power at the DC microgrid.

3.2.3. Index-Based Performance Evaluation of the Proposed Controllers

The performance of the proposed cyber security mitigation techniques has been evaluated through the voltage index calculation using the following equation [38]:

$$Voltage\ Index = \int_0^T |\Delta V_{DC}| dt \tag{12}$$

where T is the simulation time for different cases. The lower the value of the voltage index, the better the system's performance. In other words, the lower the deviation of the *DC* grid terminal voltage with respect to time, the greater the system's stability. For an obvious understanding of the controller performance, we have calculated the percentage improvement following the equation below:

$$\frac{V_{index\,No\ controller} - V_{index\,With\ controller}}{V_{index\,No\ controller}} \times 100 \tag{13}$$

Table 4 shows the voltage index values for all the scenarios that have been considered in this study. From these index values, it is evident that the cyber-attack makes the PV-connected DC microgrid very insecure, as the voltage index value without the controller is huge. Using the proposed controllers, the system's performance improved greatly. However, in all cases, it is clearly apparent from the percentage improvement data that the nonlinear controller is slightly better than the PI controller. For all the scenarios in Case-I, the proposed nonlinear controller demonstrated an average 2% improvement compared to the PI controller. Again, on the same comparison basis, a significant improvement of around 10% is evident for Case-II using the nonlinear controller. In both cases, the percentage improvements are statistically significant.

Table 4. Voltage index values for various controllers.

Attack Scenario	**Voltage Index**				
	No Controller	**Proposed Nonlinear Based Controller**		**PI Controller**	
	Index	**Index**	**Percentage Improvement (%)**	**Index**	**Percentage Improvement (%)**
Case-I Scenario 1	7.442	0.1104	98.517	0.1518	96.96
Scenario 2	3.927	0.0517	98.684	0.1511	96.15
Scenario 3	4.398	0.1140	97.41	0.1518	96.55
Case-II Scenario 1	3.763	0.0534	98.58	0.3772	89.98

4. Conclusions

This work proposes a novel solution based on a nonlinear controller to mitigate the adverse effects of cyber-attacks on various components of a DC microgrid system. Two types of cyber-attacks, i.e., distributed denial of service and false data injection, in the form of single and repetitive attacks on specific components of the microgrid system, have been considered. An index-based quantitative analysis for the proposed control method has been made. Based on the obtained simulation results, the following conclusions can be drawn:

(i) The proposed nonlinear controller-based method is effective in mitigating the adverse effects of cyber-attacks on the DC microgrid system.
(ii) The performance of the proposed controller is better than that of the PI controller.
(iii) Due to the simplicity of the proposed solution, it can easily be implemented in real practice.

It is important to note here that the proposed controller is designed for the particular power system arrangement shown in Figure 1. However, the controller is scalable and can be effective for different power systems just by re-tuning the control parameters.

To the best of our knowledge, there is no work available yet in the literature for cyber-attack mitigation in the power grid system. Hence, we approached a simplistic method of mitigation using a nonlinear controller, considering the above-mentioned advantages. In the near future, we will be more open to exploring and experimenting with other novel solutions, including artificial intelligence-based control and mitigation methods.

Author Contributions: Conceptualization, M.H.A. and S.R.A.; methodology, M.H.A. and S.R.A.; software, M.H.A. and S.R.A.; validation, M.H.A. and S.R.A.; formal analysis, M.H.A. and S.R.A.; investigation, M.H.A. and S.R.A.; resources, M.H.A. and S.R.A.; data curation, M.H.A. and S.R.A.; writing—original draft preparation, M.H.A. and S.R.A.; writing—review and editing, M.H.A.; visualization, M.H.A. and S.R.A.; supervision, M.H.A.; project administration, M.H.A.; funding acquisition, M.H.A. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: Data are contained within the article.

Acknowledgments: The authors gratefully acknowledge the financial support of the Department of Electrical and Computer Engineering at the University of Memphis, USA, to complete this work.

Conflicts of Interest: Author Sultana Razia Akhter was employed by the company American Express. The remaining authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

References

1. Saafan, A.A.; Khadkikar, V.; Moursi, M.S.E.; Zeineldin, H.H. A New Multiport DC-DC Converter for DC Microgrid Applications. *IEEE Trans. Ind. Appl.* **2023**, *59*, 601–611. [CrossRef]
2. Adly, M.; Strunz, K. Irradiance-Adaptive PV Module Integrated Converter for High Efficiency and Power Quality in Standalone and DC Microgrid Applications. *IEEE Trans. Ind. Electron.* **2018**, *65*, 436–446. [CrossRef]
3. Liu, J.; Zhang, W.; Rizzoni, G. Robust Stability Analysis of DC Microgrids With Constant Power Loads. *IEEE Trans. Power Syst.* **2018**, *33*, 851–860. [CrossRef]
4. Lotfi, H.; Khodaei, A. AC versus DC microgrid planning. *IEEE Trans. Smart Grid* **2017**, *8*, 296–304. [CrossRef]
5. Li, Z.; Shahidehpour, M.; Aminifar, F. Cybersecurity in Distributed Power Systems. *Proc. IEEE* **2017**, *105*, 1367–1388. [CrossRef]
6. Zhong, X.; Yu, L.; Brooks, R.; Venayagamoorthy, G.K. Cyber security in smart DC microgrid operations. In Proceedings of the 2015 IEEE First International Conference on DC Microgrids (ICDCM), Atlanta, GA, USA, 7–10 June 2015; pp. 86–91.
7. Kumar, M.; Srivastava, S.C.; Singh, S.N. Control Strategies of a DC Microgrid for Grid Connected and Islanded Operations. *IEEE Trans. Smart Grid* **2015**, *6*, 1588–1601. [CrossRef]
8. Li, P.; Liu, Y.; Xin, H.; Jiang, X. A Robust Distributed Economic Dispatch Strategy of Virtual Power Plant Under Cyber-Attacks. *IEEE Trans. Ind. Inform.* **2018**, *14*, 4343–4352. [CrossRef]
9. Zhang, H.; Meng, W.; Qi, J.; Wang, X.; Zheng, W.X. Distributed Load Sharing Under False Data Injection Attack in an Inverter-Based Microgrid. *IEEE Trans. Ind. Electron.* **2019**, *66*, 1543–1551. [CrossRef]
10. Liu, S.; Chen, B.; Zourntos, T.; Kundur, D.; Butler-Purry, K. A Coordinated Multi-Switch Attack for Cascading Failures in Smart Grid. *IEEE Trans. Smart Grid* **2014**, *5*, 1183–1195. [CrossRef]
11. Langer, L.; Smith, P.; Hutle, M.; Schaeffer-Filho, A. Analysing cyber-physical attacks to a Smart Grid: A voltage control use case. In Proceedings of the 2016 Power Systems Computation Conference (PSCC), Genoa, Italy, 20–24 June 2016; pp. 1–7.
12. Beg, O.A.; Johnson, T.T.; Davoudi, A. Detection of False-Data Injection Attacks in Cyber-Physical DC Microgrids. *IEEE Trans. Ind. Inform.* **2017**, *13*, 2693–2703. [CrossRef]
13. Anwar, A.; Mahmood, A.N.; Shah, Z. A Data-Driven Approach to Distinguish Cyber-Attacks from Physical Faults in a Smart Grid. In Proceedings of the 24th ACM International on Conference on Information and Knowledge Management, Melbourne, Australia, 19–23 October 2015; pp. 1811–1814.
14. Wang, H.; Ruan, J.; Wang, G.; Zhou, B.; Liu, Y.; Fu, X.; Peng, J. Deep Learning-Based Interval State Estimation of AC Smart Grids Against Sparse Cyber Attacks. *IEEE Trans. Ind. Inform.* **2018**, *14*, 4766–4778. [CrossRef]
15. Taha, A.F.; Qi, J.; Wang, J.; Panchal, J.H. Risk Mitigation for Dynamic State Estimation Against Cyber Attacks and Unknown Inputs. *IEEE Trans. Smart Grid* **2018**, *9*, 886–899. [CrossRef]
16. Zhou, Y.; Miao, Z. Cyber attacks, detection and protection in smart grid state estimation. In Proceedings of the 2016 North American Power Symposium (NAPS), Denver, CO, USA, 18–20 September 2016; pp. 1–6.

17. Kapourchali, M.H.; Sepehry, M.; Aravinthan, V. Fault Detector and Switch Placement in Cyber-Enabled Power Distribution Network. *IEEE Trans. Smart Grid* **2018**, *9*, 980–992. [CrossRef]
18. Ashok, A.; Govindarasu, M.; Ajjarapu, V. Online Detection of Stealthy False Data Injection Attacks in Power System State Estimation. *IEEE Trans. Smart Grid* **2018**, *9*, 1636–1646. [CrossRef]
19. Abdelgayed, T.S.; Morsi, W.G.; Sidhu, T.S. A New Harmony Search Approach for Optimal Wavelets Applied to Fault Classification. *IEEE Trans. Smart Grid* **2018**, *9*, 521–529. [CrossRef]
20. Majumdar, A.; Pal, B.C. Bad Data Detection in the Context of Leverage Point Attacks in Modern Power Networks. *IEEE Trans. Smart Grid* **2018**, *9*, 2042–2054.
21. Liang, G.; Weller, S.R.; Luo, F.; Zhao, J.; Dong, Z.Y. Distributed Blockchain-Based Data Protection Framework for Modern Power Systems Against Cyber Attacks. *IEEE Trans. Smart Grid* **2019**, *10*, 3162–3173. [CrossRef]
22. Farraj, A.; Hammad, E.; Kundur, D. A Cyber-Physical Control Framework for Transient Stability in Smart Grids. *IEEE Trans. Smart Grid* **2018**, *9*, 1205–1215. [CrossRef]
23. Pan, K.; Teixeira, A.; Cvetkovic, M.; Palensky, P. Cyber risk analysis of combined data attacks against power system state estimation. *IEEE Trans. Smart Grid* **2019**, *10*, 3044–3056. [CrossRef]
24. Nguyen, T.N.; Liu, B.-H.; Nguyen, N.P.; Chou, J.-T. Cyber Security of Smart Grid: Attacks and Defenses. In Proceedings of the ICC 2020—2020 IEEE International Conference on Communications (ICC), Dublin, Ireland, 7–11 June 2020; pp. 1–6. [CrossRef]
25. Ghelani, D. Cyber Security in Smart Grids, Threats, and Possible Solutions. *Preprint* **2022**.
26. Teixeira, A.; Dan, G.; Sandberg, H.; Johansson, K.H. A cyber' security study of a SCADA energy management system: Stealthy deception attacks on the state estimator. In Proceedings of the IFAC World Congress, Milan, Italy, 28 August–2 September 2011.
27. Mohammadi, F. Emerging Challenges in Smart Grid Cybersecurity Enhancement: A Review. *Energies* **2021**, *14*, 1380. [CrossRef]
28. Ghosh, S.; Ali, M.H.; Dasgupta, D. Effects of Cyber-Attacks on the Energy Storage in a Hybrid Power System. Paper ID: 18PESGM1268. In Proceedings of the IEEE PES General Meeting, Portland, OR, USA, 5–10 August 2018.
29. Li, Y.; Yan, J. Cybersecurity of Smart Inverters in the Smart Grid: A Survey. *IEEE Trans. Power Electron.* **2023**, *38*, 2364–2383. [CrossRef]
30. Asri, S.; Pranggono, B. Impact of Distributed Denial-of-Service Attack on Advanced Metering Infrastructure. *Wirel. Pers. Commun.* **2015**, *83*, 2211–2223. [CrossRef]
31. Unsal, D.B.; Ustun, T.S.; Hussain, S.M.S.; Onen, A. Enhancing Cybersecurity in Smart Grids: False Data Injection and Its Mitigation. *Energies* **2021**, *14*, 2657. [CrossRef]
32. Sahu, T.P.; Dixit, T.V. Modelling and analysis of perturb and observe and incremental conductance MPPT algorithm for PV array using Ćuk converter. *IEEE Students' Conf. Electr. Electron. Comput. Sci. SCEECS* **2014**, *4*, 213–224.
33. Farrokhabadi, M.; König, S.; Cañizares, C.A.; Bhattacharya, K.; Leibfried, T. Battery Energy Storage System Models for Microgrid Stability Analysis and Dynamic Simulation. *IEEE Trans. Power Syst.* **2018**, *33*, 2301–2312. [CrossRef]
34. Khan, S.S.; Rafiq, M.A.; Shareef, H.; Sultan, M.K. Parameter optimization of PEMFC model using backtracking search algorithm. In Proceedings of the 2018 5th International Conference on Renewable Energy: Generation and Applications (ICREGA), Al Ain, United Arab Emirates, 25–28 February 2018; pp. 323–326.
35. Arani, M.F.M.; Mohamed, Y.A.I. Assessment and Enhancement of a Full-Scale PMSG-Based Wind Power Generator Performance Under Faults. *IEEE Trans. Energy Convers.* **2016**, *31*, 728–739. [CrossRef]
36. Yan, J.; Tang, B.; He, H. Detection of false data attacks in smart grid with supervised learning. In Proceedings of the 2016 International Joint Conference on Neural Networks (IJCNN), Vancouver, BC, Canada, 24–29 July 2016; pp. 1395–1402. [CrossRef]
37. Habib, A.K.M.A.; Hasan, M.K.; Hassan, R.; Islam, S.; Thakkar, R.; Vo, N. Distributed denial-of-service attack detection for smart grid wide area measurement system: A hybrid machine learning technique. *Energy Rep.* **2023**, *9*, 638–646. [CrossRef]
38. Akhter; Razia, S. Exploring Cyber Security Issues and Solutions for Various Components of DC Microgrid System. Master's Thesis, University of Memphis, Memphis, TN, USA, 2018. Available online: https://digitalcommons.memphis.edu/etd/1860 (accessed on 14 January 2024).

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.